



Translates of completely normal elements and the Morgan-Mullen conjecture

*University of West Macedonia, Department of Mathematics Seminar
Kastoria, May 2026*

Giorgos Kapetanakis

 University of Thessaly

 kapetanakis@uth.gr

 gkapet.users.uth.gr

Outline

Motivation

A new construction of completely normal elements

Results

The translate properties and the MM property

Future work

Basic notation and concepts

- Set \mathbb{F}_q the finite field of order q , \mathbb{F}_{q^n} for its extension of degree n , and for $d \mid n$, \mathbb{F}_{q^d} the corresponding intermediate extension.
- Some $a \in \mathbb{F}_{q^n}$ is called *primitive* if it generates the multiplicative group $\mathbb{F}_{q^n}^*$. It is known that every finite field contains primitive elements, while primitive elements are important for both theoretical and practical reasons.
- Some $a \in \mathbb{F}_{q^n}$ is called q^n/q -*normal* (or *normal over \mathbb{F}_q* or just *normal*) if its \mathbb{F}_q -conjugates form an \mathbb{F}_q -basis of \mathbb{F}_{q^n} (when viewed as an \mathbb{F}_q -vector space). A basis of this form is called an q^n/q -*normal basis*.
- Some $a \in \mathbb{F}_{q^n}$ is called q^n/q -*completely normal* (or just *completely normal*) if it is q^n/q^d -normal for all $d \mid n$.

The (completely) normal basis theorem

Theorem (Normal Basis Theorem)

There exists some $a \in \mathbb{F}_{q^n}$ that is q^n/q -normal.

Initially established by Hensel (1888), later established in the more general setting of finite Galois extensions by Noether (1932) and Deuring (1933).

Theorem (Completely Normal Basis Theorem)

There exists some $a \in \mathbb{F}_{q^n}$ that is q^n/q -completely normal.

Established by Blessenohl-Johnsen (1986), Hachenberger (1994) gave a simplified proof.

The primitive normal basis theorem

A natural question is whether there exist elements of \mathbb{F}_{q^n} that combine normality and primitivity. The answer to that question was given by the following celebrated result.

Theorem (Primitive Normal Basis Theorem)

There exists some $a \in \mathbb{F}_{q^n}$ that is simultaneously primitive and q^n/q -normal.

- Initially established by Lenstra-Schoof (1987) and Cohen-Huczynska (2003) gave a computer-free proof.
- Both proofs employ the *character sum method*.
- Numerous generalizations have been considered:
Cohen-Huczynska (2010), GK (2014), GK (2014), GK-Reis (2019).

The Morgan-Mullen conjecture

A simple glimpse to the previous theorems leads to wondering about the existence of elements of \mathbb{F}_{q^n} that are, at the same time, primitive and completely normal.

Conjecture (Morgan-Mullen, 1996)

Every finite field extension possesses the MM property.

- The extension $\mathbb{F}_{q^n}/\mathbb{F}_q$ possesses the *MM property* if it contains an element $a \in \mathbb{F}_{q^n}$ that is primitive and completely normal.
- Partially established by various means, but still open.

Computational results

The most obvious method is direct verification with the help of computers.

Theorem (Morgan-Mullen, 1996)

Suppose that $q \leq 97$ and $q^n < 10^{50}$. Then $\mathbb{F}_{q^n}/\mathbb{F}_q$ possesses the MM property.

Theorem (Hachenberger-Hackenberg, 2019)

Suppose that $n \leq 202$ or $q < 10^4$ and $q^n < 10^{80}$. Then, $\mathbb{F}_{q^n}/\mathbb{F}_q$ possesses the MM property.

Completely basic extensions

If $\mathbb{F}_{q^n}/\mathbb{F}_q$ is such that every q^n/q -normal element is q^n/q -completely normal, this extension is *completely basic*.

Theorem (Blessenohl-Johnsen, 1991)

The finite field extension $\mathbb{F}_{q^n}/\mathbb{F}_q$ is completely basic if and only for every prime divisor r of n , $r \nmid d$, where d stands for the order of q modulo the relatively prime to q part of n/r .

- The MM property is immediate for completely basic extensions.
- This family includes cases such as $n = r^2$ (where r is a prime number), $n \mid q - 1$ or $n = p^k$, where k is arbitrary and $p = \text{char } \mathbb{F}_q$.

Regular extensions

- If $\gcd(n, d) = 1$, where d is the order of q modulo the square-free part of n that do not divide q , then $\mathbb{F}_{q^n}/\mathbb{F}_q$ is called a *regular extension*.
- Completely basic extensions are regular extensions.
- This family also include extensions $\mathbb{F}_{q^n}/\mathbb{F}_q$, where the set $D = \{r \mid n : r \text{ prime}\}$ satisfies
 1. $|D| = 1$, or,
 2. for every $r \in D$ we have that $r \mid q - 1$ or $r \mid q$, or,
 3. $D \subseteq \{7, 11, 13, 17, 19, 31, 41, 47, 49, 61, 73, 97, 101, 107, 109, 139, 151, 163, 167, 173, 179, 181, 193\}$.
- $\mathbb{F}_{q^n}/\mathbb{F}_q$ is regular if n is a power of a Carmichael number.

Theorem (Hachenberger, 2001, 2010, 2019)

Regular extensions possess the MM property.

General results

A combinatorial result

Theorem (Hachenberger, 2016)

Suppose that $q \geq n^{7/2}$ and $n \geq 7$, or, $q \geq n^3$ and $n \geq 37$, then $\mathbb{F}_{q^n}/\mathbb{F}_q$ possesses the MM property.

- Uses elementary combinatorial arguments.
- The proof depends on an estimate of the number of q^n/q -completely normal elements, that derives from combinatorial arguments.
- The number of q^n/q -completely normal elements is unknown and we do not even have useful estimates if n is large compared to q .

General results

A character sum result

Theorem (Garefalakis-GK, 2018)

If the part of n that is relatively prime to q is smaller than q , then $\mathbb{F}_{q^n}/\mathbb{F}_q$ possesses the MM property. In particular, all extensions $\mathbb{F}_{q^n}/\mathbb{F}_q$ with $n \leq q$ possess the MM property.

- A tweak of the character sum method was used.

General results

An improvement

Theorem (Garefalakis-GK, 2018)

If either n is odd and $n < q^{4/3}$, or, n is even, $q - 1 \nmid n$ and $n < q^{5/4}$, then $\mathbb{F}_{q^n}/\mathbb{F}_q$ possesses the MM property.

- Essentially with the same techniques as the previous result, with more emphasis given to technical details.

Some background from the proof of the CNBT

In the proof of the CNBT the following plays a vital role.

Proposition (Hachenberger, 1994)

Assume that $n = n_1 n_2$ where n_1, n_2 are relatively prime. If $a_i \in \mathbb{F}_{q^{n_i}}$ is q^{n_i}/q -completely normal for $i = 1, 2$, then $a_1 a_2$ is q^n/q -completely normal.

- Inductively, this leads to the CNBT.
- The element $a_1 a_2$ above has order at most $(q^{n_1} - 1)(q^{n_2} - 1)/(q - 1)$, i.e., it is never primitive.
- This is a key factor for the persistence of the Morgan-Mullen Conjecture.

Our generalization

An auxiliary lemma

Lemma

Suppose $a \in \mathbb{F}_{q^n}$ is q^n/q -normal and take some $c \in \mathbb{F}_q$. If $p \mid n$, then $a + c$ is q^n/q -normal. If $p \nmid n$, then the following are equivalent:

1. $a + c$ is q^n/q -normal.
2. $\text{Tr}_{q^n/q}(a + c) \neq 0$.
3. $c \neq -\text{Tr}_{q^n/q}(a) \cdot n^{-1}$, where n is seen as an element of \mathbb{F}_q .

Our generalization

An auxiliary proposition

Proposition

Assume that $n = n_1 n_2$ where n_1 and n_2 are relatively prime. If $a_i \in \mathbb{F}_{q^{n_i}}$ is q^{n_i}/q -completely normal for $i = 1, 2$. If $p \mid n$, then $a_1 a_2 + c$ is q^n/q -completely normal for every $c \in \mathbb{F}_q$. If $p \nmid n$, then, for every $c \in \mathbb{F}_q$, the following are equivalent:

1. $a_1 a_2 + c$ is q^n/q -completely normal.
2. $\text{Tr}_{q^n/q}(a_1 a_2 + c) \neq 0$.
3. $c \neq -\text{Tr}_{q^n/q}(a_1 a_2) \cdot n^{-1}$, where n is seen as an element of \mathbb{F}_q .

Our generalization

Sketch of the proof

- $a_1 a_2$ is q^n/q -completely normal.
- Fix some $c \in \mathbb{F}_q$. If $c = -n^{-1} \operatorname{Tr}_{q^n/q}(a_1 a_2)$ (in the case $p \nmid n$), $a_1 a_2 + c$ cannot be q^n/q -completely normal. So, from now on, either $p \mid n$, or $\operatorname{Tr}_{q^n/q}(a_1 a_2 + c) \neq 0$ if $p \nmid n$.
- Take some $d \mid n$. If $p \mid (n/d)$, $a_1 a_2 + c$ is q^n/q^d -normal. So, we focus on the case $p \nmid (n/d)$.
- In this case, $a_1 a_2 + c$ is q^n/q^d -normal if $\operatorname{Tr}_{q^n/q^d}(a_1 a_2 + c) \neq 0$. However, if this is not the case, then

$$\operatorname{Tr}_{q^n/q}(a_1 a_2 + c) = \operatorname{Tr}_{q^d/q} \left(\operatorname{Tr}_{q^n/q^d}(a_1 a_2 + c) \right) = \operatorname{Tr}_{q^d/q}(0) = 0,$$

a contradiction.

Translates of completely normal elements

The set of translates of $a \in \mathbb{F}_{q^n}$ is defined as $\mathcal{T}_a = \{a + c : c \in \mathbb{F}_q\}$.

Theorem

Let $\mathbb{F}_{q^n}/\mathbb{F}_q$ be a finite field extension and let $n = p_1^{n_1} \cdots p_k^{n_k}$ be the prime decomposition of n , with $k \geq 2$. Further, take some $q^{p_i^{n_i}}/q$ -completely normal a_i , for every $i = 1, \dots, k$ and set $a = a_1 \cdots a_k$.

1. If $p \mid n$, \mathcal{T}_a is comprised of q^n/q -completely normal elements.
2. If $p \nmid n$, then the set $\mathcal{T}_a \setminus \{a - \text{Tr}_{q^n/q}(a) \cdot n^{-1}\}$ (where n is seen as an element of \mathbb{F}_q), is comprised of q^n/q -completely normal elements

Proof

Inductively, $a_1 \cdots a_{k-1}$ is $q^{p_1^{n_1} \cdots p_{k-1}^{n_{k-1}}}/q$ -completely normal. Now, apply the last proposition. □

The importance of our construction

This means that instead of one q^n/q -completely normal element (that is *definitely not* primitive), we now have $q - 1$ such elements (with most of them being *possibly* primitive).

We are going to use this construction in two ways:

1. The first way gives results.
2. The second way gives hope.

Partially completely basic extensions

We introduce the following notion.

Definition

Let $\mathbb{F}_{q^n}/\mathbb{F}_q$ be an extension of finite fields, such that $n = n_1 n_2$, where $n_1, n_2 > 1$ with $\gcd(n_1, n_2) = 1$ and $\mathbb{F}_{q^{n_2}}/\mathbb{F}_q$ is completely basic. Then we call the extension (n_1, n_2) -*partially completely basic*.

- The family of partially completely basic extensions is large.
- For example, if $n = r_1^{n_1} \cdots r_k^{n_k}$ and $\mathbb{F}_{q^n}/\mathbb{F}_q$ is not completely basic, it is partially completely basic if $n_i = 1$ or 2 for some i , if $r_i = p$ for some i , or, if $r_i^{n_i} \mid q^n - 1$ for some i .
- An extension may be (n_1, n_2) -partially completely basic for multiple parameters n_1 and n_2 .

Conditions

Theorem

Let $\mathbb{F}_{q^n}/\mathbb{F}_q$ be an (n_1, n_2) -partially completely basic extension, with $p \nmid n$ and

$$\frac{q-2}{q-1} \cdot q^{n_2/2} \geq 2n_1 W(q') W(F'_{n_2}),$$

where $W(X)$ is the number of squarefree divisors of X , $q' = q^n - 1$ and $F'_{n_2} = x^{n_2} - 1 \in \mathbb{F}_{q^{n_2}}[x]$. Then $\mathbb{F}_{q^n}/\mathbb{F}_q$ possesses the MM property.

Theorem

Let $\mathbb{F}_{q^n}/\mathbb{F}_q$ be an (n_1, n_2) -partially completely basic extension, with $p \mid n$ and

$$q^{n_2/2} \geq n_1 W(q') W(F'_{n_2}).$$

Then $\mathbb{F}_{q^n}/\mathbb{F}_q$ possesses the MM property.

Notes on the proof

- We fix some $a \in \mathbb{F}_{q^{n_1}}$ that is q^{n_1}/q -completely normal and we are looking for some $b \in \mathbb{F}_{q^{n_2}}$ and $c \in \mathbb{F}_q^*$ such that b is q^{n_2}/q -normal, $ab + c$ is primitive, and $\text{Tr}_{q^n/q}(ab + c) \neq 0$. Then, observe that $ab + c$ is primitive and q^n/q -completely normal.
- We use expressions of the characteristic functions of these properties that employ characters.
- We use the following character sum estimate initially established by Fu and Wan (2014) with a simpler proof provided by Mazumder, GK, Kala, and Basnet (2025):

$$\left| \sum_{c \in \mathbb{F}_q} \chi(a + c) \psi(c) \right| \leq nq^{1/2}.$$

An asymptotic result

Preparation

Lemma (Apostol, 1976)

For every $\delta > 0$, $W(n) = o(n^\delta)$, where o signifies the little- o notation.

Lemma (Lenstra-Schoof, 1987)

Let q be a prime power and n a positive integer. Then, we have $W(F'_n) \leq 2^{\frac{1}{2}(n + \gcd(n, q-1))}$. In particular, $W(F'_n) \leq 2^n$, while the equality holds if and only if $n \mid q - 1$. Furthermore, if $n \nmid q - 1$, $W(F'_n) \leq 2^{3n/4}$.

Lemma (Aguirre-Neumann, 2021)

Let q be a prime power and n a positive integer. Then, $W(F'_n) \leq 2^{\frac{n+a}{b}}$ for some $a, b \in \mathbb{Z}$. In particular, for $q \geq 29$, we have $(a, b) = (0, 1)$; for $7 \leq q \leq 27$, we have $(a, b) = (q - 1, 2)$ and for $q \leq 5$ we have the following values for a, b :

q	a	b	q	a	b	q	a	b	q	a	b
2	14	5	3	20	4	4	12	3	5	18	3

An asymptotic result

Upon combining the previous lemmas with our conditions, we obtain:

Theorem

Let $\mathbb{F}_{q^n}/\mathbb{F}_q$ be an (n_1, n_2) -partially completely basic extension, where n_2 is large compared to n_1 , then $\mathbb{F}_{q^n}/\mathbb{F}_q$ possesses the MM property, unless n is odd and $q = 2$.

An algorithm for the MM property

Preparation

Lemma (Cohen-Huczynska, 2003)

For any $\alpha \in \mathbb{N}$ and a positive real number ν , $W(\alpha) \leq \mathcal{C}_\nu^{(\alpha)} \cdot \alpha^{1/\nu}$, where $\mathcal{C}_\nu^{(\alpha)} = \prod_{i=1}^t 2/(p_i^{1/\nu})$ and p_1, p_2, \dots, p_t are the primes less than or equal to 2^ν that divide α .

Let p_1, \dots, p_s be all the primes less or equal to 2^ν . In addition to the number $\mathcal{C}_\nu^{(\alpha)}$ defined above we will use the following two numbers:

1. $\mathcal{C}_\nu := \prod_{i=1}^s 2/(p_i^{1/\nu})$. Clearly, $\mathcal{C}_\nu^{(\alpha)} \leq \mathcal{C}_\nu$ for all $\alpha \in \mathbb{Z}$.
2. For any $1 \leq j \leq s$, $\mathcal{C}_\nu^{[p_j]} := \mathcal{C}_\nu p_j^{1/\nu} / 2$. Clearly, $\mathcal{C}_\nu^{(\alpha)} \leq \mathcal{C}_\nu^{[p_j]}$ for all $\alpha \in \mathbb{Z}$ with $p_j \nmid \alpha$.

An algorithm for the MM property I

Input: n_1

Output: **SUCCESS** or **FAIL**

Step 1 Set n_{\min} as the minimum value of n_2 that is not covered by the Hachenberger-Hackenberg computations.

Step 2 For $n_2 = n_{\min}$, find q_{\max} , the minimum q that satisfies our condition, with estimates for $W(F'_{n_2})$ and $W(q')$ (we use \mathcal{C}_{4n_1}).

Step 3 For each $3 \leq q < q_{\max}$, find the maximum value of n_2 , $n_{\max}^{(q)}$, not satisfying the condition of the previous step (we use $\mathcal{C}_{4n_1}^{[p]}$).

Step 4 For each $3 \leq q \leq q_{\max}$ we identify which $n_{\min} \leq n_2 \leq n_{\max}^{(q)}$ are such that

- $\mathbb{F}_{q^{n_2}}/\mathbb{F}_q$ is completely basic,
- $\gcd(n_1, n_2) = 1$, and
- $q^{n_1 n_2} > 10^{80}$.

An algorithm for the MM property II

- Step 5** For each pair check our condition, with $W(F'_{n_2})$ explicitly computed and $W(q')$ estimated (we use $\mathcal{C}_{4n_1}^{(q^{n_1 n_2} - 1)}$). Remove from the list of possible exceptions the pairs that pass this test.
- Step 6** For each pair check our condition, with $W(F'_{n_2})$ and $W(q')$ explicitly computed. Remove from the list of possible exceptions the pairs that pass this test.
- Step 7** If the list of possible exceptions is nonempty, return **FAIL**.
- Step 8** Repeat the previous steps for $q = 2$ with the second condition $(p \mid n)$ over the first $(p \nmid n)$.
- Step 9** If the list of possible exceptions remain nonempty, return **FAIL**. Otherwise, return **SUCCESS**.

An explicit result

We successfully applied the algorithm (on SAGEMATH) for $n_1 = 2$ and 3 and obtained partial results for $n_1 = 4$.

Theorem

Let $\mathbb{F}_{q^n}/\mathbb{F}_q$ be an (n_1, n_2) -partially completely basic extension. Then $\mathbb{F}_{q^n}/\mathbb{F}_q$ possesses the MM property in the following cases:

1. $n_1 = 2$ or 3.
2. $n_1 = 4$ and either
 - $q \geq 199211272511189639$ ($\approx 2 \cdot 10^{17}$),
 - $n_2 \geq n_1^{n_1} = 256$ and $q \geq 22271$, or,
 - $n_2 \geq n_1^6 = 4096$.

The translate properties

If for every $a \in \mathbb{F}_{q^n}$ such that $\mathbb{F}_q(a) = \mathbb{F}_{q^n}$, \mathcal{T}_a contains a primitive element, then $\mathbb{F}_{q^n}/\mathbb{F}_q$ possesses the *translate property*. If \mathcal{T}_a contains two primitive elements, $\mathbb{F}_{q^n}/\mathbb{F}_q$ possesses the *strong translate property*.

Theorem (Davenport-Carlitz, 1937, 1953)

Let n be a positive integer. There exists some $TP(n)$ such that for every prime power $q > TP(n)$, the extension $\mathbb{F}_{q^n}/\mathbb{F}_q$ possesses the translate property.

In this work we prove the strong version.

Theorem

Let n be a positive integer. There exists some $STP(n) \geq TP(n)$ such that for every prime power $q > STP(n)$, the extension $\mathbb{F}_{q^n}/\mathbb{F}_q$ possesses the strong translate property.

An interesting connection — Is it pointless?

Our construction implies the following:

Theorem

The extension $\mathbb{F}_{q^n}/\mathbb{F}_q$ possesses the MM property if, either $p \mid n$ and $q > \text{TP}(n)$, or, $q > \text{STP}(n)$.

- Little is known about the numbers $\text{TP}(n)$ and only a handful of them are known:
 - $\text{TP}(2) = 1$ (Cohen, 1983)
 - $\text{TP}(3) = 37$ (Cohen, 2009)
 - $43 \leq \text{TP}(4) \leq 102829$ (Bailey-Cohen-Sutherland-Trudgian, 2019)
 - $\text{TP}_2(2) = 41$ (Cohen-GK, 2020)
- These suggest that $\text{TP}(n)$ is significantly larger than n , hence, known results already cover the extensions that are known to possess the (strong) translate property.

Future work

- We believe that (with additional computational efforts) our concrete results can potentially be extended to $n_1 = 4$.
- Increasing n_1 further should be feasible after implementing known methods for relaxing conditions such as ours. These methods should increase n_1 to two-digit numbers.
 - Prime sieve (Cohen-Huczynska, 2003).
 - Modified prime sieve (Bailey-Cohen-Sutherland-Trudgian, 2019).
 - Hybrid bound (Bagger, 2024).
- In the literature, for example see (Aravena, 2020), one can find additional constructions of completely normal elements. These constructions could be exploited into establishing the MM property for additional finite fields extensions.

More on this problem can be found in the textbooks:



D. Hachenberger.

Finite Fields: Normal Bases and Completely Free Elements, volume 390 of *Kluwer Internat. Ser. Engrg. Comput. Sci.*

Kluwer Academic Publishers, Boston, MA, 1997.



D. Hachenberger and D. Jungnickel.

Topics in Galois fields, volume 29 of *Algorithms Comp. Math.*

Springer Nature Switzerland, Cham, 2020.




G. L. Mullen and D. Panario (eds.).

Handbook of Finite Fields, Discrete Math. Appl.

CRC Press, Boca Raton, FL, 2013.

This work can be found at

 **T. Garefalakis and G. Kapetanakis.**

Translates of completely normal elements and the
Morgan-Mullen conjecture.

arXiv:2509.23245 [math.NT], 2025.

Thank you for your attention!